



## Het gevecht tegen ongewenste e-mail

# Liever ham dan

Krijg jij ook een dagelijkse portie ongewenste e-mail binnen? Je bent niet alleen: wereldwijd blijkt maar liefst 80% van alle berichten *spam*. In dit dossier gaan we dieper in op dit fenomeen: de achtergronden, maar vooral ook de technieken om het te vermijden en uit je mailbox te lichten. CEDRIC MESKENS

Wat met een technischer term UBE (unsolicited bulk e-mail) of UCE (unsolicited commercial e-mail) heet, staat bij het grote publiek bekend als 'spam'. Spam is weliswaar de merknaam van een goedkoop, ingeblikt vleesproduct, maar de term werd na een Monty Python-sketch synoniem voor iets wat we tegen onze wil te slikken krijgen. In die sketch bleek een eettent namelijk nauwelijks iets anders te

# spam!



Monty Python: spam komt je de strot uit!

serveren dan spam (nagenieten kan op http://video.google.com/videoplay?docid=5627694446211716271). Al die ongewenste mail is vooral erg vervelend, want het betekent dagelijks weer tijdverlies. Bovendien is het soms zelfs gevaarlijk, want spammers schrikken er evenmin voor terug phishing-mails te sturen: e-mails met een valse link naar een bank of een service als eBay of PayPal, met de bedoeling je accountgegevens – en nadien je geld – te ontfutselen.

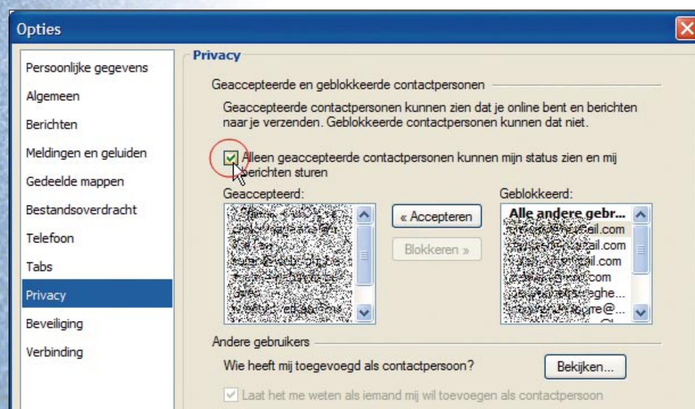
Overigens treffen we spam niet alleen aan bij e-mails, maar ook in allerlei andere vormen van internetcommunicatie. In nieuwsgroepen (usenet) heb je bijvoorbeeld EMP (excessive multiple postings), waarbij spammers talloze berichtjes naar eenzelfde nieuwsgroep posten, of ECP (excessive cross postings), waarbij eenzelfde bericht naar talrijke nieuwsgroepen wordt gepost. Een combinatie van beide zonden heet dan weer Jello. Ook op webpagina's komen we vormen van spam tegen, met de bedoeling zoekmachines – en hun gebruikers – om de tuin te leiden: het zogenaamde spamdexing. Iemand plaatst bijvoorbeeld talloze keren eenzelfde begrip – genre 'sex', 'free' en 'clickx' – in de metatags van zijn pagina's, om zo meer bezoekers te lokken. Gelukkig zijn de meeste zoekmachines hier intussen tegen gewapend. Dichter bij de 'klassieke' vorm van spam leunt een meer recent fenomeen als *spim* aan: spam over instant messaging. Zodra je je aanmeldt bij bijvoorbeeld Windows Live Messenger, verschijnen er ongewenste berichten in een pop-upvenster, zogezegd afkomstig van een van je buddies. Min of meer verwant hiermee zijn de pop-ups die spammers tot op je bureaublad krijgen door handig misbruik te maken van de in Windows ingebouwde messenger service. Maar wie SP2 heeft geïnstalleerd, hoeft daar in principe niet meer voor te vrezen, omdat die deze service standaard uitschakelt. De messenger service is trouwens niet hetzelfde als Windows Messenger.

Ook *spit* steekt stilaan de kop op. Deze term staat voor 'spam over internet telephony', en meteen weet je dat deze spammers het vooral op VoIP gemunt hebben: een technologie waarmee je tegen vaak erg voordelige tarieven kan bellen via het internet. Vooral in combinatie met *SIP* (session initation protocol) lijkt VoIP het gedroomde doelwit van telemarketeers te worden. Zo'n SIP-toestel beschikt namelijk (ook) over een uri (uniform resource identifier), een adresseringsschema dat erg goed op een e-mailadres lijkt. Wie dat te pakken krijgt, kan jou dus – erg goedkoop – opbellen...

In dit dossier focussen we ons echter op spam in de context van e-mailberichtgeving, want hiermee heeft nagenoeg elke Clickx-lezer dagelijks af te rekenen. Het vervolg van dit dossier hebben we opgesplitst in twee delen. In deel 1 komen preventieve maatregelen aan bod waarmee je in de eerste plaats kan vermijden dat spam je mailbox (en die van anderen) bereikt. In deel twee gaan we ervan uit dat spammers je e-mailadres reeds te pakken hebben, en komt het er dus op aan zo efficiënt mogelijk spam van ham (je gewenste berichten) te scheiden.




Spam: ook goedkoop, ingeblikt vlees.




IM privacyopties helpen je tegen spim te beschermen.

Services (lokaal)

Messenger

De service starten

Beschrijving:
Hiermee worden berichten tussen clients en servers uitgewisseld die met behulp van de opdracht net send of de Alerter-service zijn gestart. Deze service is niet gerelateerd aan Windows Messenger. Als deze service is gestopt, zal de Alerter-service geen berichten verzenden. Als deze service is uitgeschakeld, zullen alle services die van deze voorziening afhankelijk zijn niet kunnen worden gestart.

| Naam | Beschrijving | Status | Opstarttype | Aanmelden als |
|---|---|---|---|---|
| Intelligente achterg... | Hiermee wo... | Gestart | Automatisch | Lokaal systeem |
| iPod-service | Services vo... | Gestart | Handmatig | Lokaal systeem |
| IPSEC-services | Hiermee wo... | | Automatisch | Lokaal systeem |
| Logical Disk Manager | Hiermee wo... | Gestart | Automatisch | Lokaal systeem |
| Logical Disk Manage... | Hiermee wo... | | Handmatig | Lokaal systeem |
| Machine Debug Man... | Supports lo... | Gestart | Automatisch | Lokaal systeem |
| Messenger | Hiermee wo... | | Handmatig | Lokaal systeem |
| Messenger USN Jou... | Deze servic... | Gestart | Handmatig | Lokaal systeem |
| Microsoft Office Dia... | Microsoft O... | | Handmatig | Lokaal systeem |
| Microsoft Office Gro... | | | Handmatig | Lokale service |
| MS Software Shado... | Beheert sch... | | Handmatig | Lokaal systeem |
| MSCamSvc | | Gestart | Automatisch | Lokaal systeem |
| Net Driver HPZ12 | | Gestart | Automatisch | Lokale service |

Spammers zoeken voortdurend naar achterpoortjes.



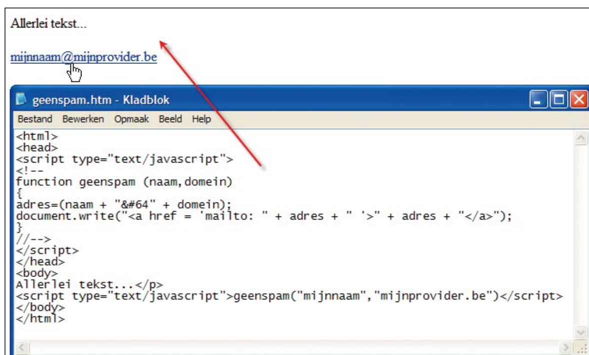

# VERMIJDEN

Voorkomen is altijd beter dan genezen... Wie erin slaagt zijn e-mailadres(sen) voor spammers verborgen te houden, zal spam weliswaar niet geheel kunnen bannen, maar het aantal ongewenste berichten toch in toom weten te houden. Het probleem is natuurlijk dat je je e-mailadres bijvoorbeeld graag op je website had opgenomen, en dat je het ook vaak nodig hebt om allerlei services te activeren. Maar met enkele trucjes omzeil je ook deze klippen...

## E-mailadres op webstek

Zodra je e-mailadres op een webstek prijkt, weten spammers het vroeg of laat wel te vinden. Die zetten daarvoor namelijk harvesting bots in: een technologie vergelijkbaar met die van zoekmachines, met dat verschil dat deze bots het gemunt hebben op e-mailadressen. Het komt er dus op aan je e-mailadres leesbaar te houden voor menselijke bezoekers, maar onzichtbaar te maken voor bots. Met een eenvoudig javascriptje heb je dat snel geregeld. Het volstaat om de volgende codesnipper op te nemen in de html-broncode van je webpagina, tussen de <head>-tags:

```
<script type="text/javascript">
<!--
function geenspam (naam,domein)
{
adres=(naam + "&#64" + domein);
document.write("a href = 'mailto: " + adres + " '>" + adres + "</a>");
}
//-->
</script>
```




*Spambots: geen kei in javascript!*

Op de plaats waar je het e-mailadres wil zien verschijnen, plaats je tussen de <body>-tags:

```
<script type="text/javascript">geenspam
("mijnnaam","mijnprovider.be")</script>
```

Je hoeft alleen maar MIJNNAAM en MIJNPROVIDER.BE te vervangen door de juiste waarden. Let er ook op dat je rechte aanhalingstekens gebruikt, dus " of ' in plaats van ” of ‘!

Schrikt dit brokje Javascript je toch wat af, gooi het dan over een andere boeg. Zo kan je de leesbare adrestekens een voor een vervangen door de overeenkomstige ISO-codes, zoals je die vindt op www.ascii.cl/htmlcodes.htm. Het adres abc@def.be zou er dan als volgt uitzien:**abc@def.b&#101**. Het is natuurlijk de vraag of spambots zich intussen ook niet in deze coderingen hebben bekwaamd. In dat geval kan je je e-mailadres nog altijd met een beeldbewerkingsprogramma als Paint uittekenen en als een afbeelding op je webpagina plaatsen. Geen grafische bolleboos? Roep dan de hulp in van het gratis tooltje XDenSer Safe Mailto www.geocities.com/xdenser/safemailto.html. Start het programma, voer je e-mailadres in en druk achtereenvolgens op **SAVE GIF** en **GET HTML**. De gegenereerde code hoef je nu alleen nog samen met het gif-plaatje in je webpagina te kleven.

## E-mailadres in nieuwsgroepen en voor aanmeldingen

Met deze trucs ben je natuurlijk weinig gebaat als je een e-mailadres moet opgeven om je bij een bepaalde nieuwsgroep of service aan te melden. Soms kom je wel weg met een vals adres, maar wat als een service bijvoorbeeld een bevestigingsmail met een bijhorende link naar het opgegeven adres stuurt? Een virtueel of wegwerpadres is de oplossing... Het komt erop neer dat je een (tijdelijk) adres aan je echte e-mailadres koppelt: alle mails die naar dat eerste adres worden gestuurd, worden dan automatisch naar het achterliggende adres doorgestuurd. Zodra je merkt dat dit doorstuuradres veel spam aankrijgt, hoef je het maar te verwijderen. Spammotel www.spammotel.com is zo'n service. Na je – gratis – aanmelding hoef je




*Een intermediair adres: snel gecreëerd, snel gewist.*

maar op de knop **CREATE A NEW ADDRESS** te drukken, en de service genereert een wegwerpadres (genre: abcdefghijkl@spammotel.com). Handig is ook dat je aan elk nieuw adres een mededeling kan hangen, zoals: adres gebruikt voor service X. Ontvang je ooit spam op dit adres, dan weet je ook meteen vanwaar de wind komt. Een vergelijkbare, gratis service is Spamgourmet www.spamgourmet.com. Hier kan je zelf aangeven hoeveel mails je maximaal op één bepaald wegwerpadres wil laten toekomen, waarna dit adres zichzelf vernietigt. En als het snel-snel moet gaan: een dienst als Yopmail vereist zelfs geen registratie. Het volstaat dat je een mail stuurt naar een willekeurigenaam@yopmail.com, waarna je achteraf via de site www.yopmail.com de mail kan checken die op dat adres is toegekomen. Minpuntje is wel dat iedereén in die mailbox kan rondneuzen.

Een alternatief is natuurlijk dat je een webmailadres creëert bij gratis diensten als Hotmail of Gmail, en een nieuw adres gebruikt zodra het vorige te veel spam ontvangt. Heb je een mailbox op overschot bij je provider, dan kan je ook die daarvoor inzetten en geregeld een ander adres verzinnen (zoals spam1@mijnprovider.be, spam2@mijnprovider.be, ...).

Hoe dan ook, ontvang je toch spamberichten, ga dan nooit in op de vraag om je uit te schrijven, "zodat je geen verdere berichtgeving meer zal




*Yopmail: digitale vuilnisbelt voor spamberichten.*

ontvangen". Vaak geef je spammers daardoor alleen maar de bevestiging dat je e-mailadres actief is, zodat er nóg meer ongewenste berichten je mailbox binnenrollen!

## Updates & antimalware

Geen spammer die nu nog jouw e-mailadres te pakken kan krijgen? Vergeet het maar... ook je eigen kennissen en vrienden durven je adres blootgeven – zonder dat ze zich van enig kwaad bewust zijn! Neen, we hebben het niet eens over de ergerlijke gewoonte om een ellenlange lijst met e-mailadressen in het CC-veld te ploffen, in plaats van het discretere BCC-veld (blind carbon copy) aan te spreken. We hebben het wél over gebruikers wiens pc als een zombie in een crimineel botnet is opgenomen. Hoe zit dat precies? Wie dacht dat spyware, trojanen of wormen nog altijd het speeltuig zijn van enkele losgeslagen whizzkids, moet zijn mening dringend herzien! Het zijn overwegend werktuigen geworden in handen van heuse maffiabendes, die zulke bollebozen inhuren. Die gaan dan op zoek naar veiligheidslekken in je systeem of browser. Zodra ze die gevonden hebben, installeren ze heimelijk malware op je toestel. Als dat gelukt is, kan je geïnfecteerde pc contact opnemen met de hackers. Op hun commando voert jouw pc dan – samen met soms duizenden andere besmette toestellen ofte zombies – zowat alles uit waar zij zin in hebben. Typische voorbeelden zijn DDoS-aanvallen (Distributed Denial of Service, waarbij getracht wordt een of andere bekende server met talloze verzoeken te overstelpen, zodat die niet langer bruikbaar is) en... het versturen van spamberichten! Zo kan het gebeuren dat je spam ontvangt van een van je kennissen, wiens pc een willoze zombie is geworden. Wil je vermijden dat ook jouw pc in zo'n crimineel botnet terecht komt, zorg er dan minstens voor dat je Windows en je browser altijd voorzien zijn van de laatste updates (veiligheidspatches). Even belangrijk is dat je een stevige firewall installeert – liefst een potiger exemplaar dan de ingebouwde firewall van Windows, zoals het gratis ZoneAlarm **www.zonelabs.com** of Comodo Firewall **www.personal-firewall.comodo.com**. Daarnaast beschik je liefst ook over een up-to-date antivirusprogramma – zoals het gratis Avast! Home Edition **www.avast.nl** of Comodo Antivirus **http://antivirus.comodo.com** – en een up-to-date antispywaretool, zoals Windows Defender **www.microsoft.com/netherlands/thuisgebruikers/beveiliging/spyware/software/default.mspx** of Ad-Aware Free **www.lavasoftusa.com**.

## HET PROTOCOL EN DE WET

Zonde eigenlijk dat we ons als arme eindgebruikers het hoofd moeten breken om spam buiten onze mailbox te houden. Kan daar juridisch geen stokje voor gestoken worden, of valt dat niet met een technische ingreep te regelen?
Beginnen we met de wet. Wie hierover alle details wil kennen, kan het boek 'Elektronische post juridisch bekeken. Praktische gids voor de onderneming en het bestuur' (Geert Somers en Jos Dumortier) raadplegen. In een notendop komt het hierop neer: de Belgische wetgever heeft binnen de Europese richtlijnen voor het zogenaamde opt-in principe gekozen. Dat houdt in dat "het gebruik van elektronische post voor reclame verboden is zonder de voorafgaande, vrije, specifieke en geïnformeerde toestemming van de geadresseerde van de boodschappen". Deze opt-in geldt echter niet als de elektronische contactgegevens onpersoonlijk zijn. Dus spam op adressen als info@ of klantendienst@ kan nog altijd, in tegenstelling tot privé-personen, die vooraf hun expliciete toestemming moeten geven. Wie in de fout gaat, riskeert € 50.000 tot € 125.000 boete. Deze regeling lijkt misschien waterdicht, maar de meeste spammers opereren vanuit het buitenland, waar de Europese – laat staan Belgische – regelgeving geen vat op heeft.



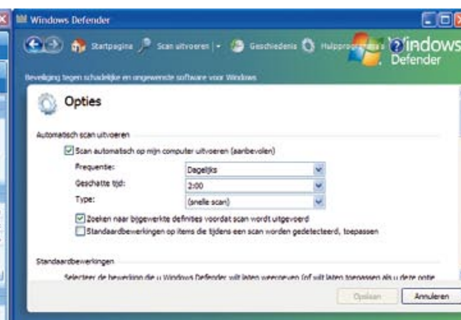

*E-mailen en de wet: dit boek vertelt er je alles over.*

Het internationale karakter van het internet speelt onze wetgeving dus parten, maar hoe zit het met de techniek? Het grote probleem is dat het SMTP-protocol (simple mail transfer protocol), gebruikt om mail te versturen, nauwelijks of geen beveiliging kent. Meer bepaald ontbeert SMTP een degelijke controle op de authenticiteit van (de afzender van) het bericht. Voor *spoofers* is het dus een koud kunstje om een mail te sturen die van iemand anders lijkt uit te gaan. Intussen wordt er wel flink gesleuteld aan een of andere vorm van 'sender authentication', oftewel een identificatie van de afzender. Denk aan Microsoft met Caller ID – dat intussen met SPF, Sender Policy Framework, is samengesmolten – en Yahoo! met DomainKeys. De eindgebruiker hoeft hier geen extra inspanningen voor te leveren, maar de providers des te meer: hun mailservers zijn dan aan een stevige upgrade toe. Komt daarbij dat ook deze schema's niet waterdicht blijken én dat mailservers hierdoor vaak ten onrechte geblokkeerd worden. Kortom: lees de rest van ons artikel toch maar grondig door...









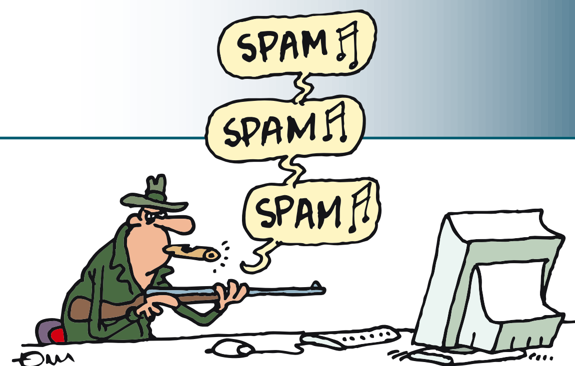

*Voor wie niet vies is van een gratis trio...*








# Filteren




OP SPAMMERS JACHT

## Standaardfilters

Oeps... de eerste spam heeft je weten te bereiken? Het wordt dus stilaan tijd voor enige actie, want voor je het weet, stroomt je mailbox vol met die ondingen. Er zit weinig anders op dan filters in te zetten, die je ham netjes van de spam weten te scheiden. Het liefst natuurlijk zonder valse negatieven – spam die abusievelijk als ham wordt aanzien – en zeker ook zonder valse positieven – ham die verkeerdelijk als spam wordt gebrandmerkt en wellicht linea recta in de snipperbak valt! Met wat geluk hoef je hier zelfs geen extra software voor in te schakelen. De meeste providers bieden namelijk een gratis antispamservice aan: veelal hoef je die maar te activeren op je persoonlijke pagina bij je provider. Vaak kan je kiezen om (vermeende) spam meteen op de mailserver te laten verwijderen of zulke berichten toch naar je mailbox door te laten sturen, weliswaar voorzien van de indicatie SPAM in de onderwerpsregel.

In dat laatste geval kan je dan een eigen filterregel in je e-mailprogramma definiëren, die zulke berichten (tijdelijk) in een aparte mailmap opslaat zodat je ze eerst nog kan checken. In Outlook Express pak je dat als volgt aan. Ga naar het menu **Extra** en kies **Berichtregels, E-mail**. Druk op de knop **Nieuw**. Selecteer achtereenvolgens **Als de regel Onderwerp bepaalde woorden bevat** en **Verplaatsen naar een bepaalde map**. Klik nu op de link **bepaalde woorden** en vul het woord SPAM in via **Toevoegen**. Klik ook de link naar een bepaalde map aan en selecteer de (nieuw gecreëerde) mailmap, bijvoorbeeld met de naam SPAM. Geef je nieuwe regel een duidelijke naam mee en bevestig met **OK** (tweemaal).

Biedt jouw provider zo'n service niet aan – foei! – dan kan je nog altijd terugvallen op de spamfilter die in je eigen e-mailprogramma, zit ingebouwd. Mailprogramma's als Outlook, Windows Mail, Thunderbird en Incredimail zijn zulke toepassingen. In Outlook 2003 activeer je die bijvoorbeeld als volgt. Ga naar het menu **Acties** en kies **Ongewenste e-mail, Opties voor ongewenste e-mail**. Kies hier **Laag** of **Hoog**, naargelang je meer valse negatieven of positieven verkiest. Puristen opteren misschien liever voor de optie **Alleen veilige lijsten** ('whitelisting'), waarbij alleen berichten van vooraf toegelaten verzenders worden doorgelaten.

Overigens voorzien de meeste e-mailprogramma's intussen ook in een andere beveiliging. Spammers stoppen namelijk regelmatig een zogenaamde webbug in hun berichten: een minuscuul onzichtbaar plaatje dat naar een externe server verwijst en hen meteen signaleert dat je e-mailadres actief is. In Outlook Express bijvoorbeeld activeer je deze bescherming als volgt: open het menu **Extra** en kies **Opties**. Ga naar het tabblad **Beveiliging** en plaats een vinkje bij **Afbeeldingen en andere externe inhoud in HTML e-mail blokkeren**.

Volstaan deze ingebouwde beveiligingsmaatregelen niet, dan grijp je wellicht beter naar zwaarder geschut...

Nieuwe e-mailregel

Selecteer eerst uw criteria en acties en geef vervolgens de waarden op in de Regelbeschrijving.

1. Selecteer de criteria voor de regel:

- [ ] Als de regel Van bepaalde personen bevat
- [x] Als de regel Onderwerp bepaalde woorden bevat
- [ ] Als de berichttekst bepaalde woorden bevat
- [ ] Als de regel Aan bepaalde personen bevat

2. Selecteer de acties voor de regel:

- [x] Verplaatsen naar een bepaalde map
- [ ] Kopiëren naar een bepaalde map
- [ ] Verwijderen
- [ ] Doorsturen naar bepaalde personen

3. Regelbeschrijving (klik op een onderstreepte waarde om deze te bewerken):

Deze regel toepassen nadat het bericht is aangekomen
Als de regel Onderwerp SPAM bevat bevat
Verplaatsen naar SPAM

4. Naam van de regel:

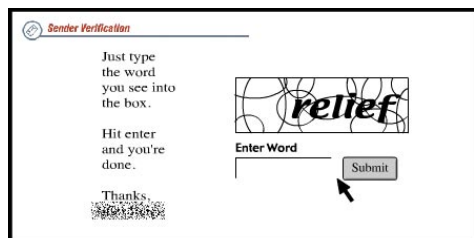
Mogelijke spam

OK Annuleren

*Met een eenvoudige filter zonder je potentiële spam tijdelijk af.*

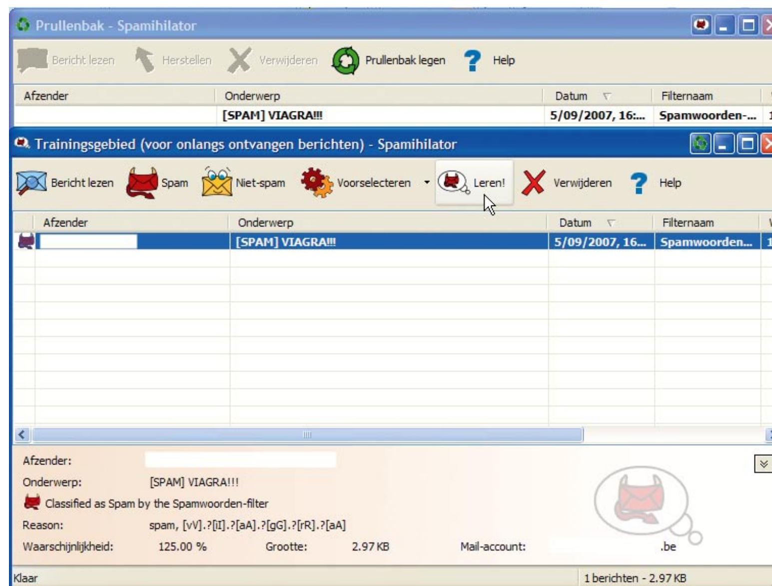
## Extra spamfilters

Er bestaan bijvoorbeeld zogenaamde challenge-response filters – een hele lijst van zulke tools vind je op **http://spamlinks.net/filter-cr.htm#filter-client-win**. Stel dat je mail ontvangt van een verzender die nog niet op je veilige lijst prijkt, dan zorgt het systeem er automatisch voor dat die verzender een mailtje ter bevestiging ontvangt (challenge). Pas als de verzender correct op dat mailtje reageert (response) – hij moet bijvoorbeeld een of ander vraagje beantwoorden of een *captcha* invullen – zal zijn oorspronkelijke bericht worden doorgelaten. In principe worden vanaf dat moment ook de volgende berichtjes van die verzender zonder meer geaccepteerd, totdat jijzelf die verzender alsnog op je zwarte lijst plaatst. Het achterliggende idee spreekt voor zich: een spammer die tienduizenden berichten verstuurt, zal nooit (kunnen) ingaan op zo'n challenge, zodat je van zulke spam gevrijwaard blijft. Uiteraard zal je bijvoorbeeld wel adressen van geautomatiseerde mailinglists op



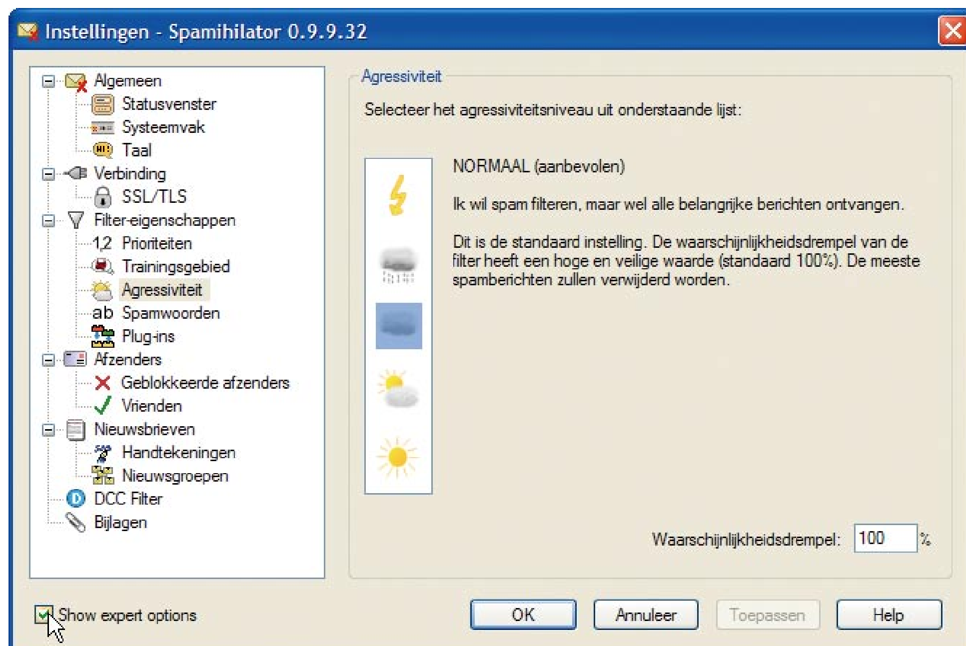

*Spam Arrest: een typisch challenge-response systeem.*

de lijst met uitzonderingen moeten plaatsen. De vraag is ook in hoeverre betrouwbare verzenders die jou voor de eerste keer een mail sturen, opgezet zullen zijn met het feit dat ze eerst nog eens op zo'n challenge moeten ingaan.
Neen, dan lijkt het ons beter dat je het bij een klassieke, maar degelijke spamfilter houdt... De betere filters zijn van het Bayesiaanse type, genoemd naar de 18de-eeuwse Britse wiskundige Thomas Bayes. Zulke filters werken met statistische analyses en zijn zelflerend. Zo geef je vooral in het begin aan zo'n filter te kennen wat ham en wat spam is. Op grond van jouw selecties leert de filter dan steeds beter zelf het onderscheid te maken, zodat je na een tijd de beslissingen van deze filters nauwelijks nog hoeft bij te sturen. Andere tools maken handig gebruik van de kracht van de online gemeenschap, en zetten een heus p2p-netwerk in om spam te identificeren (zoals DCC, Spamfighter en SpamNet). Hoe meer gebruikers berichten van een bepaalde afzender als spam markeren, hoe groter de waarschijnlijkheid dat het effectief om spam gaat en hoe strenger de filter zal oordelen.
Spamihilator www.spamihilator.com is een gratis spamfilter die beide technieken combineert: het is een volbloed Bayesiaanse filter, waarbij je ook




*Desnoods zet je Spamihilator af en toe zelf op de juiste weg.*

een DCC-plugin kan activeren. De tool nestelt zich tussen je e-mailprogramma en de mailbox bij je provider. Spamihilator controleert op de achtergrond vervolgens alle inkomende mail en speelt alleen hamberichten ongehinderd door aan het e-mailprogramma. Bij de installatie klik je bij voorkeur het plusje aan naast **Plugins**. Als je DCC niet mee wenst te installeren (omdat je bijvoorbeeld nog met een inbelverbinding het internet op gaat), verwijder je hier het vinkje. Geef ook te kennen met welk e-mailprogramma Spamihilator hoort samen te werken en welke accounts de tool moet controleren. Na afloop zie je een nieuw icoontje in de Windows-taakbalk. Klik hier met de rechtermuisknop op en kies **Settings**. Klik in de rubriek **General Settings** op de optie **Language** en selecteer **Check the Spamihilator Internet Server for new language packs**. Haal dit pack binnen en installeer het. Voortaan spreekt Spamihilator keurig (nu ja) Nederlands. We raden je aan alle instellingen, en dan vooral die binnen de rubrieken **Filter-eigenschappen** en **Afzenders**, grondig na te kijken en uit te testen. Botst Spamihilator op vermeende spamberichten, dan plaatst hij die standaard in zijn prullenbak. Je kan de inhoud hiervan op elk moment bekijken door te dubbelklikken op het icoontje. Geselecteerde berichten kan je dan alsnog lezen, of definitief verwijderen. Via de knop **Herstellen** geef je echter aan dat je het bericht toch nog wil ontvangen. De eerstvolgende keer sluist Spamihilator het bericht dan netjes door naar je e-mailprogramma. Wil je de analytische vermogens van Spamihilator versneld verfijnen, klik dan met de rechtermuisknop op het icoontje en kies **Trainingsgebied**. Hier vind je een overzicht van onlangs ontvangen berichten. Met behulp van de knoppen **Spam** en **Niet-spam** voorzie je die zelf van de gewenste markering. Druk daarna op de knop **Leren**; Spamihilator zal dan de nodige lessen trekken uit jouw selectie...
Clickx wenst je alvast veel spamvrij mailplezier! ♦




*Hoe agressief had je Spamihilator graag gewild?*

**VAKTAAL** | A - M | N - Z

**CAPTCHA:** Een test die wordt gebruikt om te bepalen of er al dan niet sprake is van een menselijke gebruiker.

**SIP:** Session Initiaton Protocol, een protocol dat multimediacommunicatie mogelijk maakt. Een bekende toepassing is bijvoorbeeld VoIP.

**SPOOFER:** Als iemand zichzelf zonder toestemming, via internet, toegang verschaft tot een computer, dan heet dat spoofing. E-mails spoofen kan door de headers van een e-mailbericht aan te passen, zodat het lijkt alsof de e-mail van iemand anders komt.